

## UNITED STATES DISTRICT COURT

for the  
District of ColumbiaIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)INFORMATION ASSOCIATED WITH THE APPLE ID  
[REDACTED]@GMAIL.COM THAT IS STORED AT  
PREMISES CONTROLLED BY APPLE, INC.Case: 17-mj-00570  
Assigned To : Howell, Beryl A.  
Assign. Date : 8/7/2017  
Description: Search and Seizure Warrant

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
of the following person or property located in the Northern District of California  
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

**YOU ARE COMMANDED** to execute this warrant on or before August 21, 2017 (not to exceed 14 days)  
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to Hon. Beryl A. Howell  
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)☐ for        days (not to exceed 30) ☐ until, the facts justifying, the later specific date of       

Date and time issued:

August 7, 2017 2:35 PMBeryl A. Howell  
Judge's signature

City and state:

Washington, DCHon. Beryl A. Howell, Chief U.S. District Judge

Printed name and title



**ATTACHMENT A**

This warrant applies to information associated with the Apple ID [REDACTED]@gmail.com that is stored at premises owned, maintained, controlled, or operated by Apple, Inc. ("Apple"), a company headquartered at 1 Infinite Loop, Cupertino, CA 95014.

**ATTACHMENT B**

**I. Information to be disclosed by Apple, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, Inc. (hereinafter “the Provider”), regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that have been deleted but are still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided

during registration, all other user names associated with the account, all account names associated with the subscriber, methods of connecting;

- f. All search history or web history;
- g. All records indicating the services available to subscribers of the accounts;
- h. All usernames associated with or sharing a login IP address or browser cookie with the accounts;
- i. All cookies, including third-party cookies, associated with the user;
- j. All records that are associated with the machine cookies associated with the user; and
- k. All telephone or instrument numbers associated with the Account (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI")).

## **II. Information to be Seized by the Government**

All information described above in Section I that constitutes evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1014 (false statements to a financial institution), 18 U.S.C. § 1344 (bank fraud), 18 U.S.C. § 1956 (money laundering), 18 U.S.C. § 951 (acting as an unregistered foreign agent), and 22 U.S.C. § 611 *et seq.* (Foreign Agents Registration Act), involving Michael Dean Cohen and occurring on or after January 1, 2016, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Communications, records, documents, and other files involving Essential Consultants, LLC;
- b. Communications, records, documents, and other files involving Bo and Abe Realty, LLC;
- c. Communications, records, documents, and other files that false representations to a financial institution with relation to intended the purpose of an account or loan at that financial institution; the nature of any business or entity associated with an

- account a financial institution; the source of funds flowing into an account; or the purpose or nature of any financial transactions involving that financial institution;
- d. Records of any funds or benefits received by or offered to Michael Dean Cohen by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
  - e. Communications, records, documents, and other files that reveal efforts by Michael Dean Cohen to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
  - f. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;
  - g. Evidence indicating the account owner's state of mind as it relates to the crimes under investigation;
  - h. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s); and
  - i. The identity of any person(s)—including records that help reveal the whereabouts of the person(s)—who communicated with the account about any matters relating to activities conducted by Michael Dean Cohen on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals.

**FILED**

## UNITED STATES DISTRICT COURT

AUG -7 2017

for the  
District of ColumbiaClerk, U.S. District and  
Bankruptcy CourtsIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)INFORMATION ASSOCIATED WITH THE APPLE ID  
[REDACTED]@GMAIL.COM THAT IS STORED AT  
PREMISES CONTROLLED BY APPLE, INC.

Case: 17-mj-00570

Assigned To : Howell, Beryl A.

Assign. Date : 8/7/2017

Description: Search and Seizure Warrant

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B. This warrant is sought pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A).

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
 18 U.S.C. § 951;  
 18 U.S.C. § 1014;  
 18 U.S.C. § 1344

Offense Description  
 Acting as a foreign agent without notice to the Attorney General;  
 False Statements to a financial institution  
 Bank Fraud

The application is based on these facts:

See attached Affidavit.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[REDACTED]

[REDACTED]

signature

Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 08/07/2017City and state: Washington, D.C.

[Signature]

Judge's signature

Hon. Beryl A. Howell, Chief U.S. District Judge

Printed name and title

**FILED**

**AUG -7 2017**

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

**Clerk, U.S. District and  
Bankruptcy Courts**

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH THE  
APPLE ID [REDACTED]@GMAIL.COM  
THAT IS STORED AT PREMISES  
CONTROLLED BY APPLE, INC.


Case: 17-mj-00570  
Assigned To : Howell, Beryl A.  
Assign. Date : 8/7/2017  
Description: Search and Seizure Warrant

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION FOR A SEARCH WARRANT**

I, [REDACTED] being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with the Apple ID [REDACTED]@gmail.com (hereinafter the “Target Account”), that is stored at premises owned, maintained, controlled, or operated by Apple, Inc. (“Apple”), a company headquartered at 1 Infinite Loop, Cupertino, CA 95014. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Attachment A. Upon receipt of the information described in Attachment A, government-authorized persons will review that information to locate the items described in Attachment B.





3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that MICHAEL DEAN COHEN has committed violations of 18 U.S.C. § 1014 (false statements to a financial institution), 18 U.S.C. § 1344 (bank fraud), 18 U.S.C. § 1956 (money laundering), 18 U.S.C. § 951 (acting as an unregistered foreign agent), and 22 U.S.C. § 611 *et seq.* (Foreign Agents Registration Act) (the “Subject Offenses”). There also is probable cause to search the information described in Attachment A for evidence, contraband, fruits, and/or instrumentalities of the Subject Offenses, further described in Attachment B.

#### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. *Id.* §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States (including a magistrate judge of such a court) . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

#### **PROBABLE CAUSE**

6. As described below, the FBI is investigating COHEN in connection with, *inter alia*, statements he made to a known financial institution (hereinafter “Bank 1”) in the course of opening a bank account held in the name of Essential Consultants, LLC and controlled by COHEN. The

FBI also is investigating COHEN in connection with funds he received from entities controlled by foreign governments and/or foreign principals, and the activities in which he engaged in the United States on their behalf without properly disclosing such relationships to the United States government.

7. On July 18, 2017, this Court, based in part on certain of the information set forth below, issued a warrant to search an email account with a different service provider, [REDACTED]@gmail.com (the “Gmail Account”), based on a finding of probable cause. On August 1, 2017, this Court, based in part on certain of the information set forth below, issued a warrant to search a second email account, mcohen@trumporg.com (the “Trump Organization Account”), based on a finding of probable cause.

8. As set forth in more detail below, there is probable cause to believe that evidence of the Subject Offenses exists in the **Target Account**, which was used by COHEN at the time of the Subject Offenses and linked to personal computing devices (including iPhones) used by COHEN. As described further below, for accounts like the **Target Account**, Apple retains records of account activity—such as the purchase of applications—as well as content from devices stored on Apple’s computers including back-ups of electronic communications and documents related to devices associated with the **Target Account**.

**A. Michael Cohen**

9. According to press reports and bank records collected during the investigation, COHEN served for over a decade as an executive in the Trump Organization, an international conglomerate with real estate and other holdings formerly controlled by President Donald Trump prior to his presidency. Until approximately January 2017, COHEN was reported to have held various positions within the Trump Organization. During an interview with *The Wall Street Journal*

in or around January 2017, COHEN described his role as being “the fix-it guy . . . . Anything that [then-President-elect Trump] needs to be done, any issues that concern him, I handle.”<sup>1</sup>

10. In or around January 2017, COHEN made public statements that he would resign from the Trump Organization to serve as the personal attorney for President Trump (serving as an attorney to the President in his personal capacity, as opposed to as a member of the White House Counsel’s Office). COHEN recently has identified himself publicly—including on his personal Twitter account—as a personal attorney for the President, and certain emails obtained pursuant to the warrant to search the Gmail Account identify Cohen as “Personal Attorney to President Donald J. Trump.”

**B. Essential Consultants, LLC**

11. In or around June 2017, federal agents reviewed information supplied by an FDIC-insured bank (“Bank 1”) based on activity that Bank 1 had observed from a number of accounts related to COHEN. According to information provided by Bank 1, COHEN has been a customer since approximately June 2011 and controls several checking and loan accounts at Bank 1, some in his personal name and others in the names of corporate entities. Agents have subsequently reviewed documents and records provided by Bank 1 related to COHEN and these various accounts.


12. Records provided by Bank 1 show that on or about October 26, 2016, COHEN opened a new checking account in the name of Essential Consultants, LLC (“Essential Consultants”); COHEN was the only authorized signatory on the account. On the paperwork associated with opening the account, COHEN listed his Trump Organization Account for contact

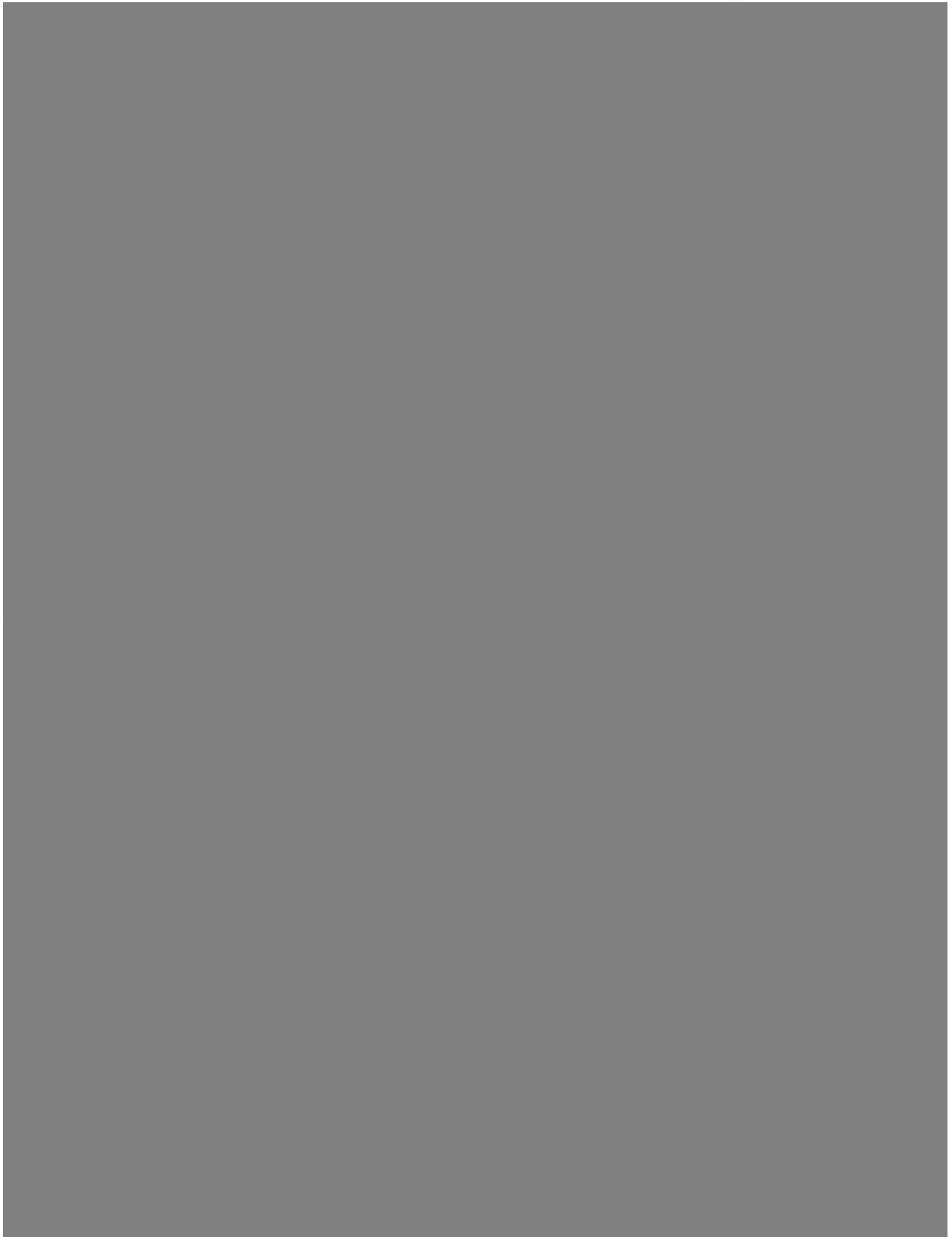
---

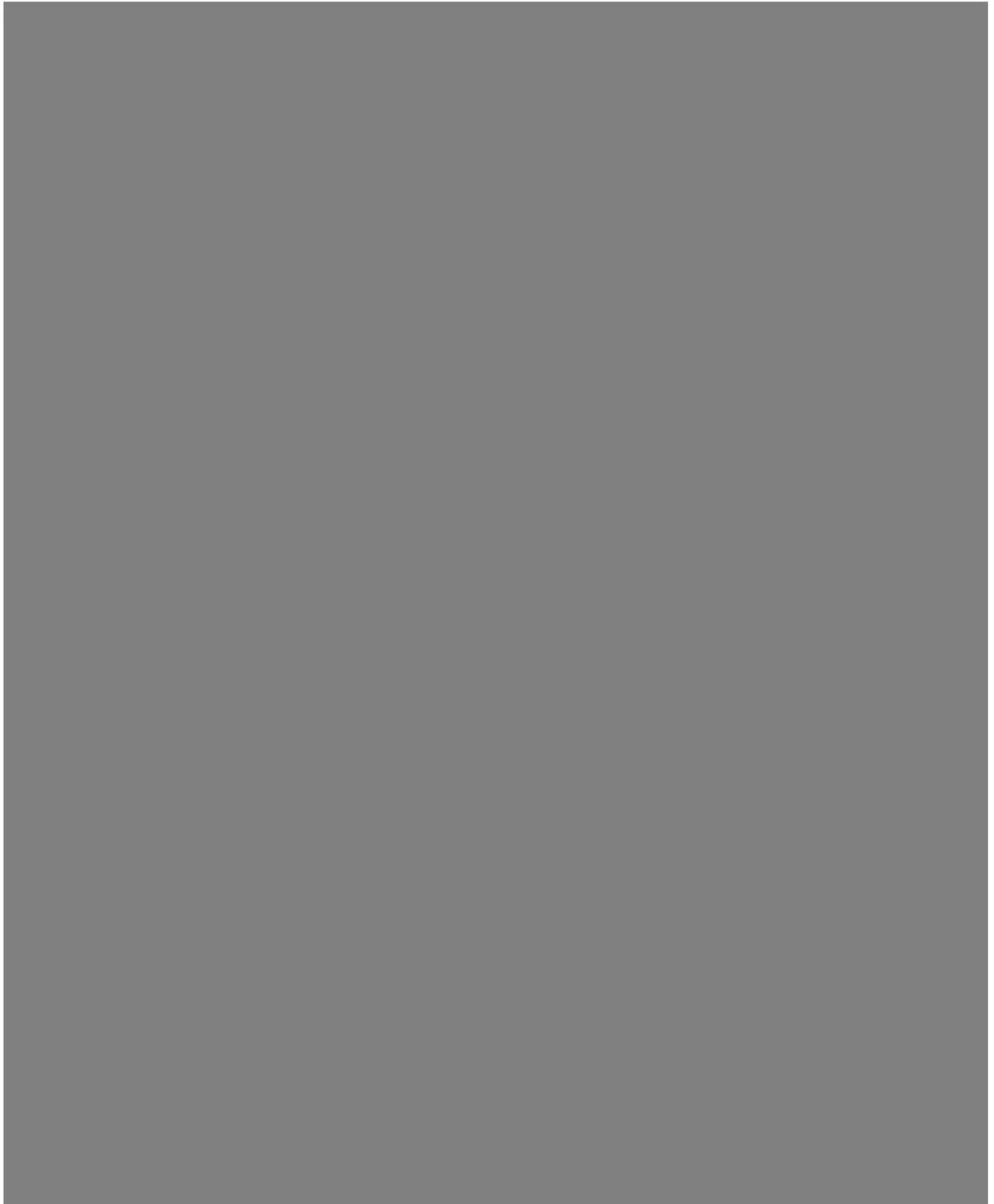
<sup>1</sup> “Intelligence Dossier Puts Longtime Trump Fixer in Spotlight,” *Wall Street Journal*, Jan. 11, 2017.

purposes. Corporate records show that Essential Consultants is a Delaware entity formed by COHEN on or about October 17, 2016.

13. According to information provided by Bank 1, when COHEN opened the Essential Consultants account, he made the following representations during the course of Bank 1's know your customer ("KYC") procedures:

- a. that he was opening Essential Consultants as a real estate consulting company to collect fees for investment consulting work;
  - b. that he intended to use his experience in real estate to consult on commercial and residential real estate deals;
  - c. that his typical clients were expected to be high net-worth domestic individuals; and
  - d. that his purpose in setting up the account was to keep the revenue from his consulting—which he said was not his main source of income—separate from his personal finances.
- 







**D. Representations to Bank 1 about Net Worth to Financial Institutions**

21. In connection with the ongoing investigation, the government has reviewed other representations COHEN has made to Bank 1 and other financial institutions, including representations regarding his net worth and financial health made during the course of loan applications. A review to date has identified substantial inconsistencies in COHEN's stated assets, liabilities, and net worth in separate loan applications submitted between 2013 and 2017.

22. For example, in or around July 2013, COHEN submitted a "Statement of Financial Condition" as of July 1, 2013 to Bank 1. The document purported to lay out COHEN's various assets and liabilities, as well as his net worth. On the document, COHEN claimed to have assets totaling approximately \$87,190,000 and liabilities of approximately \$9,550,000. On the same document, COHEN claimed to have a net worth of approximately \$70,600,000.

23. In or around October 2014, COHEN submitted a "Statement of Financial Condition" as of August 1, 2014 to Bank 1. The document purported to lay out COHEN's various assets and liabilities, as well as his net worth. On the document, COHEN claimed to have assets totaling approximately \$99,420,000 and liabilities of approximately \$23,550,000. On the same document, COHEN claimed to have a net worth of approximately \$75,870,000.

24. In or around February 2016, in connection with opening the \$500,000 HELOC described above, COHEN submitted a summary of his assets, liabilities, and net worth to Bank 1. COHEN claimed to have assets totaling approximately \$63,435,315 and liabilities of approximately \$10,419,209. On the same document, COHEN claimed to have a net worth of approximately \$53,016,106.

25. On or about June 8, 2017, COHEN sent an email from his Gmail account to an employee of a different FDIC-insured financial institution ("Bank 5") a "Statement of Financial



Condition” as of May 1, 2017.<sup>6</sup> On the document, COHEN claimed to have assets totaling approximately \$41,955,000 and liabilities of approximately \$39,130,000. On the same document, COHEN claimed to have a net worth of approximately \$2,825,000.

**E. Foreign Transactions in the Essential Consultants Account with a Russian Nexus**

26. As set forth above, in or around October 2016, COHEN made several representations to Bank 1 in connection with the bank’s KYC review process, including that he expected funds deposited into the Essential Consultants account would constitute income from his consulting work, that his consulting clients were expected to be domestic (that is, within the United States), and that he expected his clients to be U.S.-based, high-net worth individuals.

27. Records obtained from Bank 1 show substantial transactional activity that appears to be inconsistent with these KYC representations. Bank 1 records show that the account received numerous deposits from foreign businesses and entities that do not reflect the stated client profile for the residential and commercial real-estate consulting services ostensibly being provided by Essential Consultants. Moreover, public records, media reports, and other publicly available sources, as well as emails obtained pursuant to the warrant to search the Gmail Account, indicate that some of these companies have significant ties to foreign governments or are entities controlled by foreign governments.

28. A search in or around July 2017 of the U.S. Department of Justice database of all agents currently or previously registered under the Foreign Agent Registration Act (“FARA”)

---

<sup>6</sup> Bank records show that COHEN has a lending relationship with a known FDIC-insured financial institution (“Bank 5”) that uses New York taxi medallions as collateral. According to the same statement, closely held entities controlled by COHEN had approximately \$20,000,000 in notes payable to Bank 5; the debt was secured by medallions with a total market value of only \$13,950,000.

confirmed that neither COHEN nor Essential Consultants is or has been a registered agent of a foreign government.<sup>7</sup> All FARA registration is handled by the U.S. Department of Justice's National Security Division in Washington, D.C.

i. Deposits by Columbus Nova, LLC

29. Telephone records related to COHEN's cellular telephone show that on or about November 8, 2016, the day of the presidential election, a telephone registered to COHEN exchanged the first in a series of text messages with the CEO of Columbus Nova, LLC ("Columbus Nova"). Between approximately November 8, 2016 and July 14, 2017, telephone records show over 230 telephone calls and 950 text messages were exchanged between COHEN's cellular telephone and the CEO of Columbus Nova. Telephone records show no such text messages or telephone calls between COHEN's cellular telephone and the CEO of Columbus Nova prior to November 8, 2016.

30. Public records show that Columbus Nova, LLC is an investment management firm controlled by Renova Group ("Renova"), an industrial holding company based in Zurich, Switzerland. According to public news accounts, Renova is controlled by Viktor Vekselberg, a wealthy Russian national. Public news accounts also report that Vekselberg is an oligarch with various connections to Russian President Vladimir Putin who publicly met with Putin as recently as in or around March 2017.<sup>8</sup> According to the news articles, Vekselberg and Renova currently are involved in various infrastructure projects in Russia, such as the building of an airport in Rostov in advance of the 2018 FIFA World Cup, which is to be held in Russia. Vekselberg has been involved in various symbolic acts seen to be in the Russian national interest, such as the purchase

---

<sup>7</sup> The database is publicly available at <https://www.fara.gov/>.

<sup>8</sup> See, e.g., "Russia's Putin Meets Tycoon Vekselberg," *Reuters*, Mar. 14, 2017.

and repatriation of historic Faberge eggs.<sup>9</sup>

31. On or about January 10, 2017, COHEN, through his Gmail Account, received an email from the CEO of Columbus Nova with the subject "About us / Russian Union of Industrialists and Entrepreneurs." The CEO told Cohen, "This is the organization that Victor was mentioning yesterday. . . . He is the head of this international relations committee of this group. . . . Will follow up with more later."

32. On or about February 10, 2017, COHEN, through his Gmail Account, received an email from an employee of Columbus Nova, informing him that his name had been added to Columbus Nova's security list at its office building. The Columbus Nova employee also told Cohen that his office would be would be available shortly.

33. According to records obtained from Bank 1 through June 30, 2017, in the first six months of 2017, the Essential Consultants bank account received six deposits, each in the amount of \$83,333 (for a running total of \$499,998). The funds for all six deposits—five of which were wire transfers and one by check—came from an account at another bank held in the name of Columbus Nova, LLC.

34. Records obtained from the financial institution ("Bank 4") where the Columbus Nova account is located show that the funds used to pay COHEN originated from a second account in the name of Renova US Management LLC ("Renova US"). For example, on or about January 27, 2017, the Columbus Nova account at Bank 4 received a deposit of \$83,333 from an account

---

<sup>9</sup> On or about September 5, 2016, media outlets reported that Russian authorities arrested two of Vekselberg's closest associates in connection with allegations that a subsidiary had paid over \$12 million in bribes to Russian government officials. Some media accounts speculated that the arrest of Vekselberg's associates, as well as the commensurate searches of Renova's head office, were intended as a warning from the Russian government that it wanted some form of cooperation or value from Vekselberg. *See, e.g., "Another Billionaire Incurs Putin's Wrath," Bloomberg*, Sept. 6, 2016.

held in the name of Renova US. The same day, a check for \$83,333 and drawn on the Columbus Nova account at Bank 4 was made out to Essential Consultants LLC. On or about March 2, 2017, the Columbus Nova account at Bank 4 received \$83,333 from the Renova US account. The same day, the Columbus Nova account was used to \$83,333 the Essential Consultants account at Bank 1. On or about March 31, 2017, the Columbus Nova account at Bank 4 received \$83,333 from the Renova US account. The same day, the Columbus Nova account was used to wire \$83,333 to the Essential Consultants account at Bank 1. The government continues to investigate why the funds used to pay COHEN have been wired through this Columbus Nova account as opposed to coming directly from the Renova US account.

ii. Plan to Lift Russian Sanctions

35. On or about February 19, 2017, *The New York Times* published an article reporting that COHEN had been involved in distributing a proposed plan to the then-National Security Adviser, Michael T. Flynn, for the United States to lift sanctions on Russia as part of a negotiated end to the hostilities in Ukraine. The terms of the proposal appear to have been favorable to the Russians, according to *The New York Times* article.<sup>10</sup>

36. According to the article, prior to meeting with Flynn, COHEN had been approached by a Ukrainian politician ("Person 2") and a Russian-American businessman ("Person 3") who had prior business dealings with COHEN and the Trump Organization. The news report stated that Person 3 had previously been responsible for scouting deals in Russia for the Trump Organization through his company; that COHEN met personally with both Person 2 and Person 3 about the proposal; and that during the meeting with Person 3, COHEN received the written plan

---

<sup>10</sup> "A Back-Channel Plan for Ukraine and Russia, Courtesy of Trump Associates," *New York Times*, Feb. 19, 2017.

in a sealed envelope.

37. The news report further stated that COHEN confirmed that he met with Person 2 and Person 3 and received the plan in a sealed envelope, and that in or around February 2017, COHEN then traveled to the White House, met the President in the Oval Office, and left the proposal in the office occupied by then-National Security Adviser Flynn. According to the news report, COHEN stated that he was waiting for a response at the time that Flynn was forced from his post as the National Security Adviser.

38. Telephone records reviewed during the investigation show that, between January 5, 2017 and February 20, 2017, a cellular telephone registered to COHEN and a telephone registered to Person 3 exchanged approximately twenty calls. Similarly, on or about January 11, 2017, a call was exchanged between a cellular telephone registered to COHEN and a telephone registered to Flynn.

39. The United States continues to investigate if any of the payments or financial relationships described above, or other relationships described further below, were connected to COHEN's involvement in the distribution of a plan to lift Russian sanctions.

**F. Other Foreign Transactions in the Essential Consultants Account**

**i. Deposits by Korea Aerospace Industries Ltd.**

40. According to Bank 1, on or about May 10, 2017 and June 9, 2017, the Essential Consultants bank account received two deposits in the amount \$150,000 (totaling \$300,000 between the two deposits) from a bank account in Seoul, South Korea. According to documents obtained from Bank 1, the account holder from which the money was sent is Korea Aerospace Industries Ltd. ("KAI"). According to its public website, KAI is a South Korea-based company that produces and sells fixed-wing aircraft, helicopter aircraft, and satellites. Public news accounts

report that KAI has partnered with Lockheed Martin to bid later this year on a \$16 billion U.S. Air Force T-X Trainer Jet Replacement Program.

41. On or about April 28, 2017, COHEN, using the Gmail account, sent an email to another individual with the subject "K Project." In the email, COHEN attached a document purporting to be a "Consulting Agreement" between KAI and Essential Consultants LLC that was to enter into effect on May 1, 2017. The document indicates that Essential Consultants would render "consulting and advisory services, as requested" by KAI; no further information was provided regarding the nature of the consulting and advisory services to be provided. The document also indicated that KAI would pay Essential Consultants "a consulting fee of One Million Two Hundred Thousand (\$1,200,000.00) US Dollars," disbursed through eight \$150,000 installments between May 2017 and December 2017.

42. According to publicly available materials and press accounts, as well as the company's financial disclosures, the Republic of Korea (South Korea) government has significant ties to KAI. KAI itself was formed in 1999 as part of a government-led effort to consolidate South Korea's aerospace industry manufacturers into a new single entity. KAI holds the exclusive rights for all of the government's military logistics and aerospace projects.<sup>11</sup> The South Korean government, through the Korea Development Bank, is the largest shareholder in KAI and its largest debt holder.<sup>12</sup> According to information provided by Bank 1, messages related to the transfer of funds from KAI indicated that the purpose of these payments was "consulting services."

---

<sup>11</sup> See, e.g., Andrew Tylecote & Francesca Visintin, *Corporate Governance, Finance and the Technological Advantage of Nations* (2008), at 165–66; International Business Publications, *Korea South: A "Spy" Guide* (2016), at 229–31.

<sup>12</sup> KAI, Annual Report 2014, available at [https://www.koreaaero.com/upload\\_images/new\\_pdf/annual/PDF/Annual\\_report\\_eng\\_2014.pdf](https://www.koreaaero.com/upload_images/new_pdf/annual/PDF/Annual_report_eng_2014.pdf).

ii. Wire Transfers from a Kazakhstani Bank

43. On or about May 10, 2017, COHEN, using his Gmail account, sent an email to an unknown individual containing an attachment with the filename "BTA-1." The attachment contained a purported invoice for \$150,000 from Essential Consultants LLC to BTA Bank in the Republic of Kazakhstan. The invoice, identified by invoice BTA-101 referred to a "monthly consulting fee" pursuant to a "Services Agreement entered into on the 8th of May, 2017." The invoice was directed to the attention of Kenges Rakishev. Open-source records identify Rakishev as the majority shareholder of Kazkommertsbank, another Kazakhstani bank that controls BTA bank. Rakishev is also the son-in-law of Kazakhstan's ambassador to Russia.

44. According to Bank 1, on or about May 22, 2017, the Essential Consultants bank account at Bank 1 received a \$150,000 deposit from an account at Kazkommertsbank. According to Bank 1, the listed account holder at Kazkommertsbank was a second Kazakhstani bank named BTA Bank, AO. Bank 1 reported that a message accompanying the wire payment indicated that the agreement was a "monthly consulting fee as per Inv BTA-101 DD May 10, 2017 consulting agreement W/N DD 08 05 2017 CNTR W/NDD 08/05/2017."<sup>13</sup>

iii. Wire Transfers from Novartis Investments, SARL

45. Bank 1 also reported that on or about April 15, 2017 and May 15, 2017, the Essential Consultants account at Bank 1 received two deposits in the amount of \$99,800 (totaling

---

<sup>13</sup> According to press reports, BTA Bank has been mired in a multi-billion dollar fraud that implicates its former top executives. According to a *Forbes* article published in or around February 2017, for example, BTA Bank's auditors PricewaterhouseCoopers previously identified a \$10 billion discrepancy on the bank's balance sheets. Subsequent investigation by forensic accountants revealed that a unit of BTA had been used to issue billions of dollars' worth of credit for property development and other deals in Russia, Ukraine, and Belarus. The investigation also indicated that funds illicitly had been removed from the bank through shell companies set up in the names of executives' family members. See "How To Get Back A Lost \$10B: One Bank's Tale in Europe's Biggest Alleged Fraud," *Forbes*, Feb. 6, 2017.

\$199,600) from a Swiss bank account held in the name of Novartis Investments, SARL. Novartis Investments, SARL is the in-house financial subsidiary of the Swiss pharmaceutical company Novartis AG.

**G. Bo and Abe Realty, LLC**



Records show that the ultimate source of funds used to repay the HELOC funds came from a different company associated with COHEN, operating under the name Bo and Abe Realty, LLC ("Bo and Abe Realty").

48. According to records of incorporation obtained from the New York Department of State, Division of Corporations, Bo and Abe Realty LLC was incorporated on or about July 29, 2013. Documents show that the organizer was Michael Cohen and the associated business address was COHEN's residential address at 502 Park Avenue, [REDACTED] New York, NY 10022. No other agents or addresses were listed on the incorporating paperwork.

49. Bank 1 records show that on or about July 31, 2013, COHEN signed account opening documentation in order to open a bank account in the name of Bo and Abe Realty. In the





documentation, COHEN identified himself as the President of Bo and Abe Realty; the opening documentation described the purpose of the business as the “purchase of real estate.” The account opening documentation also listed two other signatories on the account: COHEN’s brother (“Person 4”), and Person 4’s mother-in-law (“Person 5”). Both Person 4 and Person 5 were identified as “members” of the company.<sup>15</sup>

#### USE AND LOCATION OF THE TARGET ACCOUNT

50. Telephone records related to COHEN suggest that in or around late September 2016, COHEN began to use a new iPhone 4S registered to the telephone number ( [REDACTED] ). This telephone number is separate from the telephone COHEN uses regularly and identifies in the signature block frequently included in emails sent from the Gmail Account. Telephone records for the telephone number [REDACTED] show that the line was subsequently used to communicate [REDACTED]

51. On or about September 28, 2016, COHEN, using his Gmail Account, received a series of emails from Apple regarding the use of the **Target Account** (identified by the Apple ID [REDACTED]@gmail.com) on a new iPhone. One such email confirmed that the **Target Account** was used to sign in to iCloud, Apple’s storage service (described further below), on an iPhone 4s.

---

<sup>15</sup> A sizeable portion of the funds deposited into the Bo and Abe Realty account came from an account in Person 5’s name. A review of documents provided by Bank 1 as well as information provided by other financial institutions indicate that both Person 4 and Person 5 are involved in and receive significant funds through a different entity operating under the name Ukrethanol, LLC (“Ukrethanol”). Ukrethanol has been involved in a series of suspicious transactions and has been suspected of possible money laundering or structuring. For example, in or around June 2013, Bank 3 closed a business account held in the name of Ukrethanol and exited its relationship with the company as a result of suspicious activity in the business account. The government continues to investigate the source of the Ukrethanol funds and the ultimate disposition of these monies.

Another email confirmed that the Target Account was used to log into the FaceTime and iMessage functions (discussed below) on an iPhone 4s.

52. On or about September 28, 2016, COHEN, using his Gmail Account, received a notification email from Apple that the **Target Account** had been used to download the application “Dust.” According to the application’s website, Dust allows users to send encrypted text messages that are not permanently stored on phones or servers. Additionally, all messages automatically erase either within twenty-four hours of being sent or as soon as they are read, depending on the settings, and the application also allows the sender to remotely erase messages from the recipient device.

53. On or about February 7, 2017, COHEN, using his Gmail Account, received a notification email from Apple that the **Target Account** had been used to download the application “WhatsApp.” According to the application’s website, WhatsApp allows users to send encrypted text messages that are not permanently stored on third-party servers.

54. On or about February 18, 2017, COHEN, using his Gmail Account, received a series of emails from Apple indicating that the **Target Account** was used to sign in to iCloud, Apple’s storage service (described further below), on a MacBook laptop. The previous day, COHEN had received a copy of an electronic receipt to his Gmail Account confirming the purchase of a new MacBook.

#### **BACKGROUND CONCERNING APPLE ID and iCloud ACCOUNTS**

55. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system. Apple provides a variety of services that can be accessed from electronic

devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, these services include email, instant messaging, and file storage:

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. Apple provides messaging and services through programs including iMessage and FaceTime, which allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.
- c. Apple provides a file hosting, storage, and sharing service called iCloud. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps. iCloud-connected services also allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user’s Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and

presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

- d. Apple allows applications and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location. Apple also allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of devices (sometimes referred to as “Find My Phone” features).
- e. Apple allows users to purchase and download digital content, applications, and other programs through its App Store and iTunes Store. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

56. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

57. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access

most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

58. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

59. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

60. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

61. Apple provides users with gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to

regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

62. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

63. The stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. For example, stored iMessage communications, voicemails, and emails may contain conversations with bank employees and foreign entities similar to those described above in COHEN's Gmail and Trump Organization accounts. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

64. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account.

Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

65. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

66. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. For instance, if there are secured and encrypted communication applications downloaded from Apple, such applications can show an attempt to hide information from investigators.<sup>16</sup> In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

67. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

---

<sup>16</sup> In this case, even if Apple does not retain content created inside these applications, records reflecting when certain applications were purchased or downloaded—for example, applications similar to the encrypted messaging services like “Dust” and “WhatsApp” applications described above—are relevant to the investigation.



**PRESERVATION OF THE TARGET ACCOUNT**

68. On or about August 7, 2017, the Federal Bureau of Investigation sent a request, pursuant to 18 U.S.C. § 2703(f), to Apple, requesting that Apple preserve all content associated with the **Target Account**.

**FILTER REVIEW PROCEDURES**

69. Review of the items described in Attachment A and Attachment B will be conducted pursuant to established procedures designed to collect evidence in a manner consistent with professional responsibility requirements concerning the maintenance of attorney-client and other operative privileges. The procedures include use of a designated “filter team,” separate and apart from the investigative team, in order to address potential privileges.

**CONCLUSION**

70. Based on the forgoing, I request that the Court issue the proposed search warrant.

*[Remainder of this page is left intentionally blank]*

**REQUEST FOR SEALING**

71. I further request that the Court order that all papers in support of this application, including the application, affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me on this 7<sup>th</sup> day of August, 2017.

A handwritten signature in cursive script, reading "Beryl A. Howell".

The Honorable Beryl A. Howell  
Chief United States District Judge

ATTACHMENT A

This warrant applies to information associated with the Apple ID [REDACTED]@gmail.com that is stored at premises owned, maintained, controlled, or operated by Apple, Inc. ("Apple"), a company headquartered at 1 Infinite Loop, Cupertino, CA 95014.

**ATTACHMENT B**

**I. Information to be disclosed by Apple, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, Inc. (hereinafter “the Provider”), regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that have been deleted but are still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided

during registration, all other user names associated with the account, all account names associated with the subscriber, methods of connecting;

- f. All search history or web history;
- g. All records indicating the services available to subscribers of the accounts;
- h. All usernames associated with or sharing a login IP address or browser cookie with the accounts;
- i. All cookies, including third-party cookies, associated with the user;
- j. All records that are associated with the machine cookies associated with the user; and
- k. All telephone or instrument numbers associated with the Account (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI").

## **II. Information to be Seized by the Government**

All information described above in Section I that constitutes evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1014 (false statements to a financial institution), 18 U.S.C. § 1344 (bank fraud), 18 U.S.C. § 1956 (money laundering), 18 U.S.C. § 951 (acting as an unregistered foreign agent), and 22 U.S.C. § 611 *et seq.* (Foreign Agents Registration Act), involving Michael Dean Cohen and occurring on or after January 1, 2016, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Communications, records, documents, and other files involving Essential Consultants, LLC;
- b. Communications, records, documents, and other files involving Bo and Abe Realty, LLC;
- c. Communications, records, documents, and other files that false representations to a financial institution with relation to intended the purpose of an account or loan at that financial institution; the nature of any business or entity associated with an

- account a financial institution; the source of funds flowing into an account; or the purpose or nature of any financial transactions involving that financial institution;
- d. Records of any funds or benefits received by or offered to Michael Dean Cohen by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
  - e. Communications, records, documents, and other files that reveal efforts by Michael Dean Cohen to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
  - f. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;
  - g. Evidence indicating the account owner's state of mind as it relates to the crimes under investigation;
  - h. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s); and
  - i. The identity of any person(s)—including records that help reveal the whereabouts of the person(s)—who communicated with the account about any matters relating to activities conducted by Michael Dean Cohen on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals.

**FILED**

**AUG - 7 2017**

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

**Clerk, U.S. District and  
Bankruptcy Courts**

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH THE  
APPLE ID [REDACTED]@GMAIL.COM  
THAT IS STORED AT PREMISES  
CONTROLLED BY APPLE, INC.

Case: 17-mj-00570  
Assigned To : Howell, Beryl A.  
Assign. Date : 8/7/2017  
Description: Search and Seizure Warrant

---

ORDER

The United States has filed a motion to seal the above-captioned warrant and related documents, including the application and affidavit in support thereof (collectively the "Warrant"), and to require Apple, Inc. ("Apple"), an electronic communication and/or remote computing services headquartered at 1 Infinite Loop, Cupertino, CA 95014 not to disclose the existence or contents of the Warrant pursuant to 18 U.S.C. § 2705(b).

The Court finds that the United States has established that a compelling governmental interest exists to justify the requested sealing, and that there is reason to believe that notification of the existence of the Warrant will seriously jeopardize the investigation, including by giving the targets an opportunity to flee from prosecution, destroy or tamper with evidence, and intimidate witnesses. *See* 18 U.S.C. § 2705(b)(2)-(5):

**IT IS THEREFORE ORDERED** that the motion is hereby **GRANTED**, and that the warrant, the application and affidavit in support thereof, all attachments thereto and other related materials, the instant motion to seal, and this Order be **SEALED** until further order of the Court; and

**IT IS FURTHER ORDERED** that, pursuant to 18 U.S.C. § 2705(b), Apple and its employees shall not disclose the existence or content of the Warrant to any other person (except attorneys for Apple for the purpose of receiving legal advice) for a period of one year or until further order of the Court.

  
\_\_\_\_\_  
THE HONORABLE BERYL A. HOWELL  
CHIEF UNITED STATES DISTRICT JUDGE

August 7, 2017  
Date



IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH THE  
APPLE ID [REDACTED]@GMAIL.COM  
THAT IS STORED AT PREMISES  
CONTROLLED BY APPLE, INC.

Case: 17-mj-00570  
Assigned To : Howell, Beryl A.  
Assign. Date : 8/7/2017  
Description: Search and Seizure Warrant

---

MOTION TO SEAL WARRANT AND RELATED DOCUMENTS AND  
TO REQUIRE NON-DISCLOSURE UNDER 18 U.S.C. § 2705(b)

The United States of America, moving by and through its undersigned counsel, respectfully moves the Court for an Order placing the above-captioned warrant and the application and affidavit in support thereof (collectively herein the "Warrant") under seal, and precluding the provider from notifying any person of the Warrant pursuant to 18 U.S.C. § 2705(b). In regard to the non-disclosure, the proposed Order would direct Apple, Inc. ("Apple"), an electronic communication and/or remote computing services provider headquartered at 1 Infinite Loop, Cupertino, CA 95014, not to notify any other person (except attorneys for Apple for the purpose of receiving legal advice) of the existence or content of the Warrant for a period of one year or until further order of the Court.

JURISDICTION AND LEGAL BACKGROUND

1. The Court has the inherent power to seal court filings when appropriate, including the Warrant. *United States v. Hubbard*, 650 F.2d 293, 315-16 (D.C. Cir. 1980) (citing *Nixon v. Warner Communications, Inc.*, 435 U.S. 589, 598 (1978)). The Court may also seal the Warrant to prevent serious jeopardy to an ongoing criminal investigation when, as in the present case, such jeopardy creates a compelling governmental interest in preserving the confidentiality of the Warrant. *See Washington Post v. Robinson*, 935 F.2d 282, 287-89 (D.C. Cir. 1991).

2. In addition, this Court has jurisdiction to issue the requested order because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court is a “district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). As discussed fully below, acts or omissions in furtherance of the offense under investigation occurred within Washington, D.C. *See* 18 U.S.C. § 3237.

3. Further, the Court has authority to require non-disclosure of the Warrant under 18 U.S.C. § 2705(b). Apple provides an “electronic communications service,” as defined in 18 U.S.C. § 2510(15), and/or “remote computing service,” as defined in 18 U.S.C. § 2711(2). The Stored Communications Act (“SCA”); 18 U.S.C. §§ 2701-2712, governs how Apple may be compelled to supply communications and other records using a subpoena, court order, or search warrant. Specifically, Section 2703(c)(2) authorizes the Government to obtain certain basic “subscriber information” using a subpoena, Section 2703(d) allows the Government to obtain other “non-content” information using a court order, and Section 2703(a)-(b)(1)(A) allows the Government to obtain contents of communications using a search warrant. *See* 18 U.S.C. § 2703.

4. The SCA does not set forth any obligation for providers to notify subscribers about subpoenas, court orders, or search warrants under Section 2703. However, many have voluntarily adopted policies of notifying subscribers about such legal requests. Accordingly, when necessary, Section 2705(b) of the SCA enables the Government to obtain a court order to preclude such notification. In relevant part, Section 2705(b) provides as follows:<sup>1</sup>

(b) Preclusion of notice to subject of governmental access. — A governmental entity acting under section 2703 . . . may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court

---

<sup>1</sup> Section 2705(b) contains additional requirements for legal process obtained pursuant to 18 U.S.C. § 2703(b)(1)(B), but the Government does not seek to use the proposed Order for any legal process under that provision.

deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

- (1) endangering the life or physical safety of an individual;
- (2) flight from prosecution;
- (3) destruction of or tampering with evidence;
- (4) intimidation of potential witnesses; or
- (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

18 U.S.C. § 2705(b). The United States District Court for the District of Columbia has made clear that a nondisclosure order under Section 2705(b) must be issued once the Government makes the requisite showing about potential consequences of notification:

The explicit terms of section 2705(b) make clear that if a courts [*sic*] finds that there is reason to believe that notifying the customer or subscriber of the court order or subpoena may lead to one of the deleterious outcomes listed under § 2705(b), the court must enter an order commanding a service provider to delay notice to a customer for a period of time that the court determines is appropriate. Once the government makes the required showing under § 2705(b), the court is required to issue the non-disclosure order.

*In re Application for Order of Nondisclosure Pursuant to 18 U.S.C. § 2705(b) for Grand Jury Subpoena #GJ2014031422765*, 41 F. Supp. 3d 1, 5 (D.D.C. 2014).

5. Accordingly, this motion to seal sets forth facts showing reasonable grounds to command Apple not to notify any other person (except attorneys for Apple for the purpose of receiving legal advice) of the existence of the Subpoena for a period of one year or until further order of the Court.

#### FACTS SUPPORTING SEALING AND NON-DISCLOSURE

6. At the present time, law enforcement officers of the FBI are conducting an investigation into violations related to 18 U.S.C. § 1014 (false statements to a financial institution), 18 U.S.C. § 1344 (bank fraud), 18 U.S.C. § 1956 (money laundering), 18 U.S.C. § 951 (acting as an unregistered foreign agent), and 22 U.S.C. § 611 *et seq.* (Foreign Agents Registration Act)

arising out of the conduct of Michael D. Cohen. It does not appear that Cohen is currently aware of the nature and scope of the ongoing FBI investigation into him.

REQUEST FOR SEALING AND NON-DISCLOSURE

7. In this matter, the government requests that the Warrant be sealed until further order of the Court and that Apple and its employees be directed not to notify any other person of the existence or content of the Warrant (except attorneys for Apple for the purpose of receiving legal advice) for a period of one year or until further order of the Court. Such an order is appropriate because the Warrant relates to an ongoing criminal investigation, the full scope of which is neither public nor known to the targets of the investigation, and its disclosure may alert these targets to the ongoing investigation and its scope. Once alerted to this investigation, potential targets would be immediately prompted to destroy or conceal incriminating evidence, alter their operational tactics to avoid future detection, and otherwise take steps to undermine the investigation and avoid future prosecution. In particular, given that they are known to use electronic communication and remote computing services, the potential target could quickly and easily destroy or encrypt digital evidence relating to their criminal activity.

8. Given the complex and sensitive nature of the criminal activity under investigation, and also given that the criminal scheme may be ongoing, the Government anticipates that this confidential investigation will continue for the next year or longer. However, should circumstances change such that court-ordered nondisclosure under Section 2705(b) becomes no longer needed, the Government will notify the Court and seek appropriate relief.

9. There is, therefore, reason to believe that notification of the existence of the Warrant will seriously jeopardize the investigation, including by giving the targets an opportunity to flee from prosecution, destroy or tamper with evidence, and intimidate witnesses. *See* 18 U.S.C.

§ 2705(b)(2)-(5). Because of such potential jeopardy to the investigation, there also exists a compelling governmental interest in confidentiality to justify the government's sealing request. *See Robinson*, 935 F.2d at 287-89.

10. Based on prior dealings with Apple the United States is aware that, absent a court order under Section 2705(b) commanding Apple not to notify anyone about a legal request, it is Apple's policy and practice, upon receipt of a warrant seeking the contents of electronically stored wire or electronic communications for a certain account, to notify the subscriber or customer of the existence of the warrant prior to producing the material sought.

WHEREFORE, for all the foregoing reasons, the government respectfully requests that the above-captioned warrant, the application and affidavit in support thereof, and all attachments thereto and other related materials be placed under seal, and furthermore, that the Court command Apple not to notify any other person of the existence or contents of the above-captioned warrant (except attorneys for Apple for the purpose of receiving legal advice) for a period of one year or until further order of the Court.

Respectfully submitted,

ROBERT S. MUELLER, III  
Special Counsel

Dated: 8/7/2017



SEP 08 2017

Clerk, U.S. District & Bankruptcy  
Courts for the District of Columbia

Case: 17-mj-00570  
Assigned To : Howell, Beryl A.  
Assign. Date : 8/7/2017  
Description: Search and Seizure Warrant

# SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California  
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

**YOU ARE COMMANDED** to execute this warrant on or before August 21, 2017 (not to exceed 14 days)  
☒ in the daytime 6:00 a.m. to 10:00 p.m.     ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Beryl A. Howell  
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (*check the appropriate box*)

☐ for \_\_\_\_\_ days (not to exceed 30)      ☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

Date and time issued:

August 7, 2017 2:35 PM

*Brya A. Howell*  
Judge's signature

City and state:

Washington, DC

Hon. Beryl A. Howell, Chief U.S. District Judge

Printed name and title



AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

**Return**

Case No.:

17-MJ-00570

Date and time warrant executed:

8/7/2017 4:58pm

Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:


On 8/22/2017 Apple provided the FBI a .gpg file titled 17087087\_Production.zip which contained 2.95 gb of encrypted data. After review and processing by FBI Cyber, the investigation team has a partial return of iCloud including data related to bookmarks, calendars, contacts, notes, finding friends, photos, and recovered documents. The complete set of data is still being processed by FBI Cyber.

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date:

9/8/2017


  
 Printed name and title

**ATTACHMENT A**

This warrant applies to information associated with the Apple ID [REDACTED] **@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Apple, Inc. ("Apple"), a company headquartered at 1 Infinite Loop, Cupertino, CA 95014.



**ATTACHMENT B**

**I. Information to be disclosed by Apple, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, Inc. (hereinafter “the Provider”), regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that have been deleted but are still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided

during registration, all other user names associated with the account, all account names associated with the subscriber, methods of connecting;

- f. All search history or web history;
- g. All records indicating the services available to subscribers of the accounts;
- h. All usernames associated with or sharing a login IP address or browser cookie with the accounts;
- i. All cookies, including third-party cookies, associated with the user;
- j. All records that are associated with the machine cookies associated with the user; and
- k. All telephone or instrument numbers associated with the Account (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI")).

## **II. Information to be Seized by the Government**

All information described above in Section I that constitutes evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1014 (false statements to a financial institution), 18 U.S.C. § 1344 (bank fraud), 18 U.S.C. § 1956 (money laundering), 18 U.S.C. § 951 (acting as an unregistered foreign agent), and 22 U.S.C. § 611 *et seq.* (Foreign Agents Registration Act), involving Michael Dean Cohen and occurring on or after January 1, 2016, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Communications, records, documents, and other files involving Essential Consultants, LLC;
- b. Communications, records, documents, and other files involving Bo and Abe Realty, LLC;
- c. Communications, records, documents, and other files that false representations to a financial institution with relation to intended the purpose of an account or loan at that financial institution; the nature of any business or entity associated with an



- account a financial institution; the source of funds flowing into an account; or the purpose or nature of any financial transactions involving that financial institution;
- d. Records of any funds or benefits received by or offered to Michael Dean Cohen by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
  - e. Communications, records, documents, and other files that reveal efforts by Michael Dean Cohen to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
  - f. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;
  - g. Evidence indicating the account owner's state of mind as it relates to the crimes under investigation;
  - h. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s); and
  - i. The identity of any person(s)—including records that help reveal the whereabouts of the person(s)—who communicated with the account about any matters relating to activities conducted by Michael Dean Cohen on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals.